ABSTRACT OF THE DISCLOSURE

An asymmetrical cryptographic method of protecting an electronic chip against fraud in transactions between the electronic chip and an application, involving calculating an authentication value V from input parameters in the electronic chip. The chip produces a pseudo-random number r specific to the transaction by means of a serial pseudo-random generator included in the chip. The chip sends the application a parameter x calculated by the application prior to the transaction, linked to the random number r by a mathematical relationship, and stored in a data memory of the chip. The chip calculates a parameter y constituting the whole or a portion of the authentication value V by means of a serial function whose input parameters are at least the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys. The chip sends the authentication value V to the application, and the application verifies the authentication value V by means of a verification function whose input parameters consist exclusively of public parameters including at least the public key p.